Improved Upper Bounds on the Hermite and KZ Constants

Jinming Wen* †, Xiao-Wen Chang‡ and Jian Weng*
* College of Information Science and Technology and the College of Cyber Security, Jinan University,
Guangzhou, 510632, China (E-mail:jinming.wen@mail.mcgill.ca, cryptjweng@gmail.com)
†State Key Laboratory of Information Security, Institute of Information Engineering,
Chinese Academy of Sciences, Beijing 100093
‡School of Computer Science, McGill University, Montreal, H3A 0E9, Canada (E-mail: chang@cs.mcgill.ca)

Abstract—**The Korkine-Zolotareff (KZ) reduction is a widely used lattice reduction strategy in communications and cryptography. The Hermite constant, which is a vital constant of lattice, has many applications, such as bounding the length of the shortest nonzero lattice vector and orthogonality defect of lattices. The KZ constant can be used in quantifying some useful properties of KZ reduced matrices. In this paper, we first develop a linear upper bound on the Hermite constant and then use the bound to develop an upper bound on the KZ constant. These upper bounds are sharper than those obtained recently by the first two authors. Some examples on the applications of the improved upper bounds are also presented.**

Index Terms—**KZ reduction, Hermite constant, KZ constant.**

I. Introduction

The lattice generated by a matrix $\boldsymbol{A} \in \mathbb{R}^{m\times n}$ with full-column rank is defined by

$$\mathcal{L}(\boldsymbol{A}) = \{\boldsymbol{A}\boldsymbol{x} \,|\, \boldsymbol{x} \in \mathbb{Z}^n\}. \tag{1}$$

The column vectors of $\boldsymbol{A}$ and n represent the basis and dimension of $\mathcal{L}(\boldsymbol{A})$, respectively.

A matrix $\boldsymbol{Z} \in \mathbb{Z}^{n\times n}$ satisfying $|\det(\boldsymbol{Z})| = 1$ is said to be unimodular. For any unimodular $\boldsymbol{Z} \in \mathbb{Z}^{n\times n}$, $\mathcal{L}(\boldsymbol{A}\boldsymbol{Z})$ is the same lattice as $\mathcal{L}(\boldsymbol{A})$. Lattice reduction is the process of finding a unimodular $\boldsymbol{Z}$ such that the column vectors of $\boldsymbol{A}\boldsymbol{Z}$ are short. There are a few types of lattice reduction strategies. The Lenstra-Lenstra-Lovász (LLL) reduction and the Korkine-Zolotareff (KZ) reduction are two of the most popular ones, and they have crucial applications in many domains including communications [1] and cryptography [2].

For efficiency, the LLL reduction is often used to preprocess the matrix $\boldsymbol{A}$ when a closest vector problem (CVP), which is defined as

$$\min_{\boldsymbol{x}\in\mathbb{Z}^n} \|\boldsymbol{y} - \boldsymbol{A}\boldsymbol{x}\|_2,$$

needs to be solved. In some communications applications, a number of CVPs with the same matrix $\boldsymbol{A}$ but different $\boldsymbol{y}$ need to be solved. In this situation, for efficiency, instead of the LLL reduction, the KZ reduction is applied to preprocess $\boldsymbol{A}$. The reason is that although it is more time consuming to perform the KZ reduction than the LLL reduction, the reduced matrix of the KZ reduction has better properties than the one obtained by the LLL reduction, and hence the total computational time of solving these CVPs by using the KZ reduction may be less than that of using the LLL reduction. Furthermore, the KZ reduction finds applications in successive integer-forcing linear receiver design [3] and integer-forcing linear receiver design [4].

It is interesting to quantify the performance of the KZ reduction in terms of shortening the lengths of the lattice vectors and reducing the orthogonality defects of the basis matrices of lattices. The KZ constant, defined by Schnorr in [5], is a measure of the quality of KZ reduced matrices. It can be used to bound the lengths of the column vectors of KZ reduced matrices from above [6], [7]. In addition to this, the KZ constant has applications in bounding the decoding radius and the proximity factors of KZ-aided successive interference cancellation (SIC) decoders from below [7]–[9]. Although the KZ constant is an important quantity, there is no formula for it. Fortunately, it has several upper bounds [5], [10], [7]. The first main aim of this paper is to improve the sharpest existing upper bound presented in [7].

The Hermite constant can be used to quantify the length of the shortest nonzero vector of lattices. Since estimating the length of the shortest vector in a lattice is a NP-hard problem [11], this application of Hermite constant is of vital importance. It also has applications in bounding the KZ constant from above [5]. Furthermore, it can be used to derive lower bounds on the decoding radius of the LLL-aided SIC decoders [7], [9], and upper bounds on the orthogonality defect of KZ reduced matrices [6], [7], [12]. Although the Hermite constant is important, its exact values are known for dimension $1 \leq n \leq 8$ and $n = 24$ only. Thus, its upper bound for arbitrary integer n is needed. In the above applications, the Hermite constant's linear upper bounds play crucial roles. Hence, in addition to the nonlinear upper bound [13], several linear upper bounds on the Hermite constant have been proposed in [6], [14], [15]. The second main aim of this paper is to improve the sharpest available linear upper bound provided in [7].

The reminder of the paper is organized as follows. Sections

This work was partially supported by NSERC of Canada grant RGPIN-2017-05138, NNSFC (No. 11871248), and the Fundamental Research Funds for the Central Universities (No. 21618329).

II and III develop a new linear upper bound on the Hermite constant and a new upper bound on the KZ constant, respectively. Finally, this paper is summarized in Section IV.

Notation. Let $\mathbb{R}^{m\times n}$ and $\mathbb{Z}^{m\times n}$ be the spaces of the $m\times n$ real matrices and integer matrices, respectively. Boldface lowercase letters denote column vectors and boldface uppercase letters denote matrices. For a matrix $\boldsymbol{A}$, we use a_{ij} to denote its (i,j) entry. $\Gamma(n)$ denotes the Gamma function.

II. A sharper linear bound on the Hermite constant

This section develops a new linear upper bound on the Hermite constant. that is sharper than [7, Theorem 1] when $n \geq 109$.

We first introduce the definition of the Hermite constant. Denote the set of $m\times n$ real matrices with full-column rank by $\mathbb{R}^{m\times n}_n$. The Hermite constant γ_n is defined as

$$\gamma_n = \sup_{\boldsymbol{A}\in\mathbb{R}^{m\times n}_n} \frac{(\lambda(\boldsymbol{A}))^2}{(\det(\boldsymbol{A}^T\boldsymbol{A}))^{1/n}},$$

where $\lambda(\boldsymbol{A})$ represents the length of a shortest nonzero vector of $\mathcal{L}(\boldsymbol{A})$, i.e.,

$$\lambda(\boldsymbol{A}) = \min_{\boldsymbol{x}\in\mathbb{Z}^n\setminus\{\boldsymbol{0}\}} \|\boldsymbol{A}\boldsymbol{x}\|_2.$$

Although the Hermite constant is a vital important constant of lattices, the values of γ_n are known only for $n=1,\ldots,8$ [16] and $n=24$ [17] (see also [7, Table 1]). Fortunately, there are some upper bounds on γ_n for any n in the literature and the sharpest one is

$$\gamma_n \leq \frac{2}{\pi}(\Gamma(2+n/2))^{2/n}, \tag{2}$$

given by Blichfeldt [13].

As explained in Section I, linear upper bounds on γ_n are very useful. There are several linear upper bounds: $\gamma_n \leq \frac{2}{3}n$ (for $n\geq 2$) [6]; $\gamma_n \leq 1+\frac{n}{4}$ (for $n\geq 1$) [14, p.35] and $\gamma_n \leq \frac{n+6}{7}$ (for $n \geq 2$) [15]. The most recent linear upper bound on γ_n is

$$\gamma_n < \frac{n}{8}+\frac{6}{5},\ \ n\geq 1, \tag{3}$$

given in [7, Theorem 1].

The following theorem gives a new linear upper bound on γ_n, which is sharper than (3) when $n\geq 109$.

Theorem 1. *For $n \geq 1$,*

$$\gamma_n < \frac{n}{8.5}+2. \tag{4}$$

Proof. By (2), to show (4), it suffices to show

$$\left(\Gamma\left(2+\frac{n}{2}\right)\right)^{2/n} < \frac{\pi(n+17)}{17},$$

which is equivalent to

$$\Gamma\left(2+\frac{n}{2}\right) < \left(\frac{\pi(n+17)}{17}\right)^{n/2}. \tag{5}$$

Then, to show (4), it is equivalent to show that

$$\phi(t) := \frac{\left[\frac{\pi}{8.5}(t+8.5)\right]^t}{\Gamma(2+t)} > 1$$

for $t=0.5,1,1.5,2,2.5,\ldots$.

By some direct calculations, one can show that

$$\phi(t)>1,\ \text{ for } t=0.5,1.5,2,2.5,\ldots,310.$$

Thus, to show (4), we only need to show that $\phi(t)$ or $\bar{\phi}(t) := \ln(\phi(t))$ is monotonically increasing when $t\geq 310$.

By some direct calculations, we have

$$\bar{\phi}'(t) = \ln\left[\frac{\pi}{8.5}(t+8.5)\right] + \frac{t}{t+8.5} - \psi(t+2),$$

where $\psi(t+2)$ is the digamma function, i.e., $\psi(t+2) = \Gamma'(t+2)/\Gamma(t+2)$. Then, to show (4), we only need to show that $\bar{\phi}'(t)\geq 0$ when $t\geq 310$. To achieve this, we use the following inequality from [18, eq. (1.7) in Lemma 1.7]:

$$\psi(t+2) \leq \ln(t+e^{1-\gamma}),\ \text{ for } t\geq 0, \tag{6}$$

where $\gamma = \lim_{n\to\infty}(-\ln n + \sum_{k=1}^n 1/k)$, which is referred to as Euler's constant. Then, from the expression of $\bar{\phi}'(t)$ given before, we have

$$\bar{\phi}'(t) \geq \rho(t),$$

where

$$\begin{aligned}\rho(t) :&= \ln\left[\frac{\pi(t+8.5)}{8.5}\right] + \frac{t}{t+8.5} - \ln(t+e^{1-\gamma})\\ &= \ln(t+8.5) - \frac{8.5}{t+8.5} - \ln(t+e^{1-\gamma}) + \ln\frac{\pi e}{8.5}.\end{aligned}$$

Since

$$\begin{aligned}\rho'(t) &= \frac{1}{t+8.5} + \frac{8.5}{(t+8.5)^2} - \frac{1}{t+e^{1-\gamma}}\\ &= \frac{(t+8.5)(t+e^{1-\gamma}) + 8.5(t+e^{1-\gamma})}{(t+8.5)^2(t+e^{1-\gamma})}\\ &\quad - \frac{(t+8.5)^2}{(t+8.5)^2(t+e^{1-\gamma})}\\ &= \frac{e^{1-\gamma}t - (72.25-17e^{1-\gamma})}{(t+8.5)^2(t+e^{1-\gamma})},\end{aligned}$$

and $\gamma < 0.58$ [19], $\rho'(t)\geq 0$ when $t>31$ as

$$\begin{aligned}&e^{1-\gamma}t - (72.25-17e^{1-\gamma})\\ >&31\times e^{1-\gamma} - (72.25-17e^{1-\gamma}) > 0.\end{aligned}$$

Thus, for $t\geq 310$, we have

$$\bar{\phi}'(t) \geq \rho(t) \geq \rho(310) > 0.0000796 > 0,$$

where the third inequality follows form the fact that $\gamma > 0.57$ [19]. □

By some simple calculations, one can easily see that the upper bound (4) is sharper than the upper bound (3) when $n\geq 109$. When $n \leq 108$, (3) is sharper than (4), but their difference is small. By the Stirling's approximation for Gamma function, the right-hand side of (2) is asymptotically $\frac{n}{\pi e} \approx \frac{n}{8.54}$. Thus, the linear bound given by (4) is very close to the nonlinear upper bound given by (2). To clearly show the improvement of (4) over (3) and how close (4) is to (2), in Figure 1 we plot the ratios of the two bounds to Blichfeldt's bound given by (2):

$$\text{Ratio 1} = \frac{\frac{n}{8}+\frac{6}{5}}{\frac{2}{\pi}(\Gamma(2+n/2))^{2/n}}, \quad \text{Ratio 2} = \frac{\frac{n}{8.5}+2}{\frac{2}{\pi}(\Gamma(2+n/2))^{2/n}}.$$

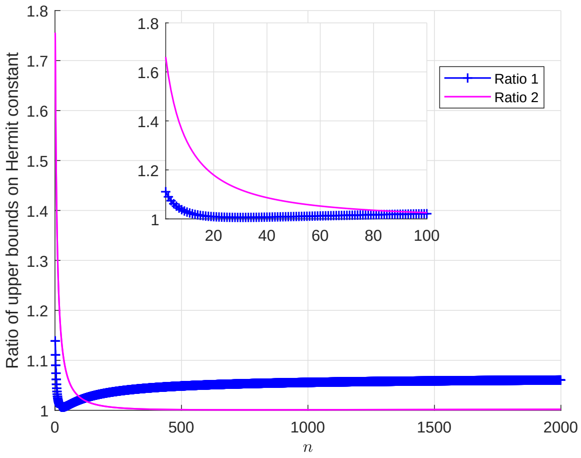

Fig. 1. The ratio of the bounds given by (4) and (3) to Blichfeldt's bound in (2) versus n

From Figure 1, one can see that the upper bound given by (4) is very close to the nonlinear upper bound given by (2), and (4) improves (3) for $n \geq 109$.

In the following, we give some remarks.

Remark 1. *The approach used by the proof for* (4) *is different from that for* (3) *used in [7]. To show* (3)*, it suffices to show (cf.* (5)*)*

$$\Gamma\left(2+\frac{n}{2}\right) < \left(\frac{\pi(n+9.6)}{16}\right)^{n/2}. \tag{7}$$

The proof for (7) *first gives an upper bound on* $\Gamma\left(2+\frac{n}{2}\right)$ *and then shows the right-hand side of* (7) *is larger than this upper bound, while the proof for* (5) *here shows* $\phi(t)$ *is a monotonically increasing function by using an upper bound on the digamma function (see* (6)*).*

Remark 2. *The improved linear upper bound* (4) *on* γ_n *can be used to improve the lower bound on the decoding radius of the LLL-aided SIC decoder that was given in [7], which is an improvement of the one given in [9, Lemma 1]. Since the derivation for the new lower bound on the decoding radius is straightforward by following the proof of [9, Lemma 1] and using* (4)*, we do not provide details.*

Remark 3. *The improved linear upper bound* (4) *on* γ_n *can be used to improve the upper bound on the orthogonality defect of KZ reduced matrices that was presented in [7, Theorem 4]. Note that the orthogonality defect of a matrix is a good measure of the orthogonality of the matrix and hence it is often used in characterizing the quality of a LLL or KZ reduced matrix.*

III. A SHARPER BOUND ON THE KZ CONSTANT

In this section, we develop an upper bound on the KZ constant that is sharper than that given by [7, Theorem 2].

We first briefly introduce the definition of the KZ reduction. Suppose that $\boldsymbol{A}$ in (1) has the following thin QR factorization (see, e.g., [20, Chap. 5]):

$$\boldsymbol{A} = \boldsymbol{Q}\boldsymbol{R}, \tag{8}$$

where $\boldsymbol{Q} \in \mathbb{R}^{m\times n}$ has orthonormal columns and $\boldsymbol{R} \in \mathbb{R}^{n\times n}$ is nonsingular upper triangular, and they are respectively referred to as $\boldsymbol{A}$'s Q-factor and R-factor. If $\boldsymbol{R}$ in (8) satisfies:

$$|r_{ij}| \leq \frac{1}{2}|r_{ii}|, \quad 1 \leq i \leq j-1 \leq n-1, \tag{9}$$

$$|r_{ii}| = \min_{\boldsymbol{x}\,\in\,\mathbb{Z}^{n-i+1}\setminus\{\boldsymbol{0}\}} \|\boldsymbol{R}_{i:n,i:n}\boldsymbol{x}\|_2, \quad 1 \leq i \leq n, \tag{10}$$

then $\boldsymbol{A}$ and $\boldsymbol{R}$ are said to be KZ reduced. Given $\boldsymbol{A} \in \mathbb{R}^{m\times n}_n$, the KZ reduction is the process of finding a unimodular matrix $\boldsymbol{Z} \in \mathbb{Z}^{n\times n}$ such that $\boldsymbol{A}\boldsymbol{Z}$ is KZ reduced.

Let $\mathcal{B}_{KZ}$ denote the set of all $m\times n$ KZ reduced matrices with full-column rank. The KZ constant is defined as [5]

$$\alpha_n = \sup_{\boldsymbol{A}\in\mathcal{B}_{KZ}} \frac{(\lambda(\boldsymbol{A}))^2}{r_{nn}^2}, \tag{11}$$

where $\lambda(\boldsymbol{A})$ denotes the length of the shortest nonzero vector of $\mathcal{L}(\boldsymbol{A})$, and r_{nn} is the last diagonal entry of the R-factor $\boldsymbol{R}$ of $\boldsymbol{A}$ (see (8)).

As explained in Section I, the KZ constant is an important quantity for characterizing some properties of KZ reduced matrices. However, its exact value is unknown. Hence, it is useful to find a good upper bound on it. Schnorr in [5, Corollary 2.5] proved that

$$\alpha_n \leq n^{1+\ln n}, \quad \text{for } n \geq 1;$$

Hanrot and Stehlé in [10, Theorem 4] showed that

$$\alpha_n \leq n\prod_{k=2}^{n} k^{1/(k-1)} \leq n^{\frac{\ln n}{2}+\mathcal{O}(1)}, \quad \text{for } n \geq 2;$$

Based on the exact value of γ_n for $1 \leq n \leq 8$ and the upper bound on γ_n in (3) for $n \geq 9$, Wen and Chang in [7, Theorem 2] showed that

$$\alpha_n \leq 7\left(\frac{1}{8}n+\frac{6}{5}\right)\left(\frac{n-1}{8}\right)^{\frac{1}{2}\ln((n-1)/8)}, \quad \text{for } n \geq 9. \tag{12}$$

In the following theorem we provide a new upper bound on α_n for $n \geq 109$, which is sharper than that in (12) for $n \geq 111$. The new bound on α_n is based on the new upper bound on the Hermite constant γ_n (4), which is sharper than that in (3) for $n \geq 109$.

Theorem 2. *The KZ constant α_n satisfies*

$$\alpha_n \leq 8.1\left(\frac{n}{8.5}+2\right)\left(\frac{2n-1}{17}\right)^{\frac{1}{2}\ln((2n-1)/17)}, \quad \textit{for } n \geq 109. \tag{13}$$

To prove Theorem 2, we need to introduce two lemmas. The first one is from [7, Lemma 2].

Lemma 1. *For $a > b > 0$ and $c > 0$*

$$\int_a^b \frac{\ln(1+c/t)}{t}dt \leq \frac{9}{8}\ln\frac{b(3a+2c)}{a(3b+2c)} + \frac{c(b-a)}{4ab}. \tag{14}$$

The second lemma which is needed for proving Theorem 2 is as follows:

Lemma 2. *Suppose that $f(t)$ satisfies $f''(t) \geq 0$ for $t \in [a,b]$. Then*

$$(b-a)f\left(\frac{a+b}{2}\right) \leq \int_a^b f(s)ds. \tag{15}$$

Proof. The left hand side of (15) is referred to as the midpoint rule for approximating the integral on the right hand side in numerical analysis. It is well known that

$$\int_a^b f(s)ds - (b-a)f\left(\frac{a+b}{2}\right) = \frac{1}{24}(b-a)^3 f''(z) \tag{16}$$

for some $z \in (a,b)$. This formula can be easily proved as follows. By Taylor's theorem,

$$\begin{aligned} f(s) =& f\left(\frac{a+b}{2}\right) + f'\left(\frac{a+b}{2}\right)\left(s - \frac{a+b}{2}\right) \\ &+ \frac{1}{2}f''(\zeta(s))\Big(s - \frac{a+b}{2}\Big)^2, \end{aligned}$$

where $\zeta(s)$ depends on $s \in (a,b)$. Integrating both sides of the above equality over $[a,b]$ and using the Mean-Value-Theorem for Integrals immediately lead to (16). Then using the condition that $f''(t) \geq 0$ for $t \in [a,b]$, we obtain (15). □

In the following, we give a proof for Theorem 2 by following the proof of [7, Theorem 2].

Proof. According to the proof of [5, Cor. 2.5],

$$\alpha_n \leq \gamma_n \prod_{k=2}^{n} \gamma_k^{1/(k-1)}. \tag{17}$$

By [7, (53)], we have

$$\prod_{k=2}^{8} \gamma_k^{1/(k-1)} = 2^{\frac{827}{420}} 3^{-\frac{8}{15}}. \tag{18}$$

By (3), we obtain

$$\prod_{k=9}^{108} \gamma_k^{1/(k-1)} \leq \prod_{k=9}^{108}\left(\frac{k}{8}+\frac{6}{5}\right)^{1/(k-1)} < 79.06. \tag{19}$$

In the following, we use Theorem 1 to bound $\prod_{k=109}^{n} \gamma_k^{1/(k-1)}$ from above. By Theorem 1, we obtain

$$\begin{aligned} \prod_{k=109}^{n} \gamma_k^{1/(k-1)} &\leq \prod_{k=109}^{n}\left(\frac{k}{8.5}+2\right)^{1/(k-1)} \\ &= \prod_{k=108}^{n-1}\left(\frac{k+18}{8.5}\right)^{1/k} \\ &= \exp\left[\sum_{k=108}^{n-1}\frac{1}{k}\ln\left(\frac{k+18}{8.5}\right)\right] \\ &\overset{(a)}{\leq} \exp\left(\sum_{k=108}^{n-1}\int_{k-0.5}^{k+0.5}\frac{1}{t}\ln\left(\frac{t+18}{8.5}\right)dt\right) \\ &= \exp\Big(\int_{107.5}^{n-0.5}\frac{1}{t}\ln\left(\frac{t+18}{t}\frac{t}{8.5}\right)dt\Big) \\ &= \exp\Big(\int_{107.5}^{n-0.5}\frac{1}{t}\ln\left(1+\frac{18}{t}\right)dt\Big) \\ &\quad \times \exp\Big(\int_{107.5}^{n-0.5}\frac{\ln(t/8.5)}{t}dt\Big), \end{aligned} \tag{20}$$

where (a) follows from Lemma 2 with $a = k-0.5, b = k+0.5$ and the fact that for $t \geq 107.5$, $\omega(t) := \frac{1}{t}\ln\left(\frac{t+18}{8.5}\right)$ satisfies

$$\begin{aligned} \omega''(t) =& \frac{1}{t^3(t+18)^2}\left(2(t+18)^2\ln\left(\frac{t+18}{8.5}\right) - (3t^2+36t)\right) \\ \geq& \frac{1}{t^3(t+18)^2}\left(2(t+18)^2 \cdot \ln\frac{125.5}{8.5} - (3t^2+36t)\right) \\ \geq& \frac{1}{t^3(t+18)^2}\left(2(t+18)^2 \cdot 2 - (3t^2+36t)\right) \geq 0. \end{aligned}$$

Now we bound the two factors on the right-hand side of (20) from above. By Lemma 1, we obtain

$$\begin{aligned} &\exp\left(\int_{107.5}^{n-0.5}\frac{1}{t}\ln\left(1+\frac{18}{t}\right)dt\right) \\ \leq\ &\exp\left(\frac{9}{8}\ln\frac{358.5(n-0.5)}{107.5(3(n-0.5)+36)} + \frac{18(n-108)}{430(n-0.5)}\right) \\ \leq\ &\exp\left(\frac{9}{8}\ln\frac{358.5(n-0.5)}{107.5\times 3(n-0.5)} + \frac{18(n-108)}{430(n-108)}\right) \\ =\ &\left(\frac{119.5}{107.5}\right)^{9/8}\exp\left(\frac{9}{215}\right). \end{aligned} \tag{21}$$

By a direct calculation, we have

$$\begin{aligned} &\exp\left(\int_{107.5}^{n-0.5}\frac{\ln(t/8.5)}{t}dt\right) \\ =\ &\exp\left(\frac{\ln^2((n-0.5)/8.5)}{2} - \frac{\ln^2(107.5/8.5)}{2}\right) \\ =\ &\left(\frac{n-0.5}{8.5}\right)^{\frac{1}{2}\ln((n-0.5)/8.5)}\left(\frac{8.5}{107.5}\right)^{\frac{1}{2}\ln(107.5/8.5)} \end{aligned} \tag{22}$$

Then combining (17)-(22) and (4), we obtain that for $n \geq 109$

$$\begin{aligned} \alpha_n \leq\ & 79.06 \times 2^{\frac{827}{420}} 3^{-\frac{8}{15}}\left(\frac{119.5}{107.5}\right)^{9/8}\exp\left(\frac{9}{215}\right) \\ &\times\left(\frac{8.5}{107.5}\right)^{\frac{1}{2}\ln\frac{107.5}{8.5}}\left(\frac{n}{8.5}+2\right)\left(\frac{n-0.5}{8.5}\right)^{\frac{1}{2}\ln(\frac{n-0.5}{8.5})} \\ <\ &(8.0911\cdots)\left(\frac{n}{8.5}+2\right)\left(\frac{n-0.5}{8.5}\right)^{\frac{1}{2}\ln(\frac{n-0.5}{8.5})} \end{aligned}$$

$$< 8.1\left(\frac{n}{8.5}+2\right)\left(\frac{2n-1}{17}\right)^{\frac{1}{2}\ln((2n-1)/17)}.$$

□

Remark 4. *Note that although the proof of Theorem 2 is similar to the proof of [7, Theorem 2], there is some difference between them. The main difference between them is (a) in* (20)*. Here, we use Lemma 2 to build (a), while the proof of [7, Theorem 2] uses the decreasing property of the integrand to get the inequality.*

To clearly see the improvement of (13) over (12), we draw the ratio of the right-hand side of (13) to that of (12) for $n = 111 : 1 : 1000$ in Figure 2. The figure shows that (13) significantly outperforms (12), and the improvement becomes more significant as n gets larger.

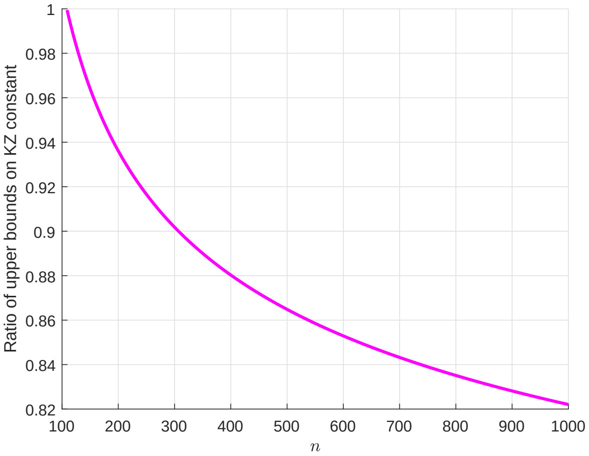

Fig. 2. The ratio of the bound given by (13) to the bound given by (12) versus n

In the following we give remarks about some applications of Theorem 2.

Remark 5. *As in [7, Remark 2], we can use the improved upper bound* (13) *on* α_n *to derive upper bounds on the proximity factors of the KZ-aided SIC decoder and these new bounds are sharper than those given in [7, Remark 2]. Since the derivations are straightforward, we omit its details.*

Remark 6. *We can use* (13) *and follow the proof of [9, Lemma 1] to derive a lower bound on the decoding radius of the KZ-aided SIC decoder, which is tighter than that given in [7, Remark 3] when* $n \geq 111$.

Remark 7. *By following the proof of [7, Theorem 3] and using* (13)*, we can also develop new upper bounds on the lengths of the KZ reduced matrices, which are tighter than those given in [7, Theorem 3] when* $n \geq 111$.

IV. Summary

The KZ reduction is one of the most popular lattice reduction methods and has many important applications. The Hermite constant is a basic constant of lattice. In this paper, we first developed a new linear upper bound on the Hermite constant and then utilized the bound to develop a new upper bound on the KZ constant. These bounds are sharper than those developed in [7]. Some applications of the new sharper bounds on the Hermite and KZ constants were also discussed.

References

[1] E. Agrell, T. Eriksson, A. Vardy, and K. Zeger, “Closest point search in lattices,” *IEEE Trans. Inf. Theory*, vol. 48, no. 8, pp. 2201–2214, 2002.

[2] D. Micciancio and O. Regev, *Lattice-Based Cryptography*. Bernstein, D. J. and Buchmann, J. (eds.), Berlin: Springer Verlagem, 2008.

[3] O. Ordentlich, U. Erez, and B. Nazer, “Successive integer-forcing and its sum-rate optimality,” in *2013 51st Annual Allerton Conference onCommunication, Control, and Computing (Allerton)*. IEEE, 2013, pp. 282–292.

[4] A. Sakzad, J. Harshan, and E. Viterbo, “Integer-forcing MIMO linear receivers based on lattice reduction,” *IEEE Trans. Wireless Commun.*, vol. 12, no. 10, pp. 4905–4915, 2013.

[5] C. P. Schnorr, “A hierarchy of polynomial time lattice basis reduction algorithms,” *Theoret. Comput. Sci.*, vol. 53, pp. 201–224, 1987.

[6] J. C. Lagarias, H. Lenstra, and C. P. Schnorr, “Korkin-zolotarev bases and successive minima of a lattice and its reciprocal lattice,” *Combinatorica*, vol. 10, no. 4, pp. 333–348, 1990.

[7] J. Wen and X.-W. Chang, “On the KZ reduction,” *IEEE Trans. Inf. Theory*, vol. 65, no. 3, pp. 1921–1935, March 2019.

[8] C. Ling, “On the proximity factors of lattice reduction-aided decoding,” *IEEE Trans. Signal Process.*, vol. 59, no. 6, pp. 2795–2808, 2011.

[9] L. Luzzi, D. Stehlé, and C. Ling, “Decoding by embedding: Correct decoding radius and DMT optimality,” *IEEE Trans. Inf. Theory*, vol. 59, no. 5, pp. 2960–2973, May 2013.

[10] G. Hanrot and D. Stehlé, “Worst-case Hermite-Korkine-Zolotarev reduced lattice bases,” *arXiv preprint arXiv:0801.3331*, 2008.

[11] M. Ajtai, “Generating hard instances of lattice problems,” in *Proc. 28th Annu. ACM Symp. Theory Comput.* ACM, 1996, pp. 99–108.

[12] S. Lyu and C. Ling, “Boosted KZ and LLL algorithms,” *IEEE Trans. Signal Process.*, vol. 65, no. 18, pp. 4784–4796, Sept 2017.

[13] H. F. Blichfeldt, “A new principle in the geometry of numbers, with some applications,” *Trans. Amer. Math. Soc.*, vol. 15, no. 3, pp. 227–235, 1914.

[14] P. Q. Nguyen and B. Vallée, Eds., *The LLL Algorithm, Survey and Applications*. Springer, 2010.

[15] A. Neumaier, “Bounding basis reduction properties,” *Des. Codes Cryptogr*, vol. 84, no. 1-2, pp. 237–259, 2017.

[16] J. Martinet, *Perfect lattices in Euclidean spaces*. Springer Science & Business Media, 2013, vol. 327.

[17] H. Cohn and A. Kumar, “The densest lattice in twenty-four dimensions,” *Electron. Res. Announc. Amer. Math. Soc.*, vol. 10, no. 7, pp. 58–67, 2004.

[18] N. Batir, “Inequalities for the gamma function,” *Arch. Math.*, vol. 91, pp. 554–563, 2008.

[19] D. H. Lehmer, “Euler constants for arithmetical progressions,” *Acta Arith*, vol. 27, no. 1, pp. 125–142, 1975.

[20] G. Golub and C. Van Loan, “Matrix Computations, 4th,” *Johns Hopkins*, 2013.